TRANSNAV
http://www.transnav.eu

the International Journal
on Marine Navigation
and Safety of Sea Transportation

Volume 17
Number 3
September 2023

DOI: 10.12716/1001.17.03.24

State-Sponsored and Organized Crime Threats to Maritime Transportation Systems in the Context of the Attack on Ukraine

R. Cichocki
Gdynia Maritime University, Gdynia, Poland

ABSTRACT: Due to its strategic importance and vast impact on the world economy, maritime transport has become a cyber battlefield. Cybersecurity organizations across the world notice and analyze adversaries such as Bear from Russia, Panda from China, Buffalo from Vietnam, Chollima from North Korea (DPRK), and others from Columbia, India, Turkey, and Iran, as well as hacktivist and E-Crime. In 2014 - 2023, Ukraine became the object of massive cyberattacks aimed at its political, social, and economic destabilization. This situation changes the perception of cyberspace and its importance for ensuring the security of the global economy, in particular, the maritime economy. Reports published by the US Coast Guard show that. In this publication, the author reviews the cybersecurity threat landscape targeting the maritime industry and transportation systems and analyzes the technics, tactics, and procedures (TTPs) used by threat actors.

1 INTRODUCTION

Cyberattacks on Ukraine have been a significant issue in recent years, with various serious incidents that show the increasing impact of such attacks. In 2014 – 2023 [1]–[3], Ukraine became the object of massive cyberattacks aimed at its political, social, and economic destabilization. On the other hand, Russian cyber operations have been relatively unsophisticated, and the threat actors used well-known malware [3]. The visibility of the actions of hackers was consequently very high. Unfortunately, that doesn't mean they were unsuccessful, especially in the first attack stage in February 2022. For this reason, it is worth noting that in the annual US Coast Guard Cyber Trends and Insights in the Marine Environment 2021 Report, the most disturbing of the finds were: easily crackable passwords, open mail relay or unsupported (vulnerable) OS or non-essential use of elevated access [4]. On many marine units, one can still find systems (ECDIS) based on Windows XP or Windows 7 operating systems [5] vulnerable to EternalBlue CVE-2017-0144 and other RCE class vulnerabilities. That indicates how much must be done to achieve maritime cyber resiliency.

On the other hand, the security measures created today quickly turn out to be both necessary, required, and insufficient. On August 20, 2019, Microsoft announced that one simple action could prevent 99,9% of attacks on user accounts – mentioning Multi-Factor Authentication [6]. Today – four years later we know at least a few technics to bypass or break MFA, such as Evilginx2 (proxy), Pass the Cookie (cookie stealing), many technic to steal SMS-based tokens, or attacking software tokens like Google Authenticator or RSA's SecureID Authenticate by utilizing one of the recent significant zero-days found in Androids and iOS devices, and last but not least Hafnium zero-day exploit which targeted server side to disable MFA altogether [7], [8].

All those facts show that the game between cybercriminals, often state-sponsored or financially motivated, and cybersecurity teams is a constant and unequal struggle.

2 UKRAINE ATTACKS

Russian APT groups carried out multi-level attacks on Ukraine in January 2022. On January 14, 2022, about seventy government websites were hacked. Kyiv claims that attackers appear to have used the software administration rights of a third-party company that developed the sites. However, it is worth mentioning that these sites utilize the Octobercms CMS system, which was vulnerable to CVE-2021-32648, discovered on May 2021, and allows attackers to gain access to user accounts through specially crafted password reset requests [9]. The DEV-0586 group conducted the second and parallel destructive malware attack on January 13 against the government, army, defense ministry, and significant banks. Wiper, known as WisperGate, was used again on February 23 against multiple Ukrainian organizations such as the financial, defense, aviation, and IT sector. ESET reported this malware as HermeticWiper, named for its genuine code signing certificate. On February 15, an extensive DDoS attack brought down the websites of the defense ministry, the army, and the most prominent Ukrainian banks: PrivatBank and Oschadbank [10]. On February 24, the Viasat KA-SAT hack was conducted and was intended to disrupt the Ukrainian military network, which used the Viasat network to provide communication services. Ten thousand previously online modems actively dropped connection and did not attempt to reconnect again. Investigation and forensic analysis show that threat actors exploit a misconfiguration in the VPN appliance to gain access to the internal management network segment of KA-SAT systems. Subsequent lateral movement through a trusted network allows the attacker to gain access to the segment allowing it to send management commands to thousands of modems simultaneously [11]. The last stage of the first quarter of 2022 begins on March 6, when Russia significantly increases the frequency of cyber-attacks against Ukrainian civilians and refugees in Poland. Only two organizations – Quad9 and Packet Clearing House, both protecting against attack by observing DNS traffic and blocking queries that show signs of attacks, reported interception and mitigation of 4,6 million attacks against computers, both Ukrainian and Polish (70% of refugees took refuge in Poland) [12].

3 APT AND THREAT LANDSCAPE

In 2014, Kevin Mandia, Senior Vice President of MANDIANT the RSA Conference first time, publicly spoke about the Chines government and military attacks against US commercial corporations. He stated that when the technological protection and controls are more sophisticated, the attack vector shifts and targets humans as the weakest link [13]. That statement was true as far back as 1979 when Kevin Mitnick most wanted FBI computer criminal gained access to Digital Equipment Corporation (DEC). The term social engineering was invented by Mitnick, who said that he always hacks the people, not the technology. This same principle applies nowadays. The last two years' FBI IC3 reports show [14] that the most dangerous attacks in terms of losses caused are those human targeted: Business Email Compromise/Email Account Compromise, Personal Data Breach, Identity Theft, and Government Impersonation. Attacks described in FBI IC3 Report cover a broad cyber landscape, including network attacks, critical infrastructure attacks, large-scale fraud schemes, and threats to national security.

Mandiant M-Trends 2022 special reports [2] show that this year the time between the attacker gaining access to the victim system and detection of its presence is decreasing from 24 days in 2020 to 21 days in 2021. However, this is only good news according to the cybersecurity landscape.

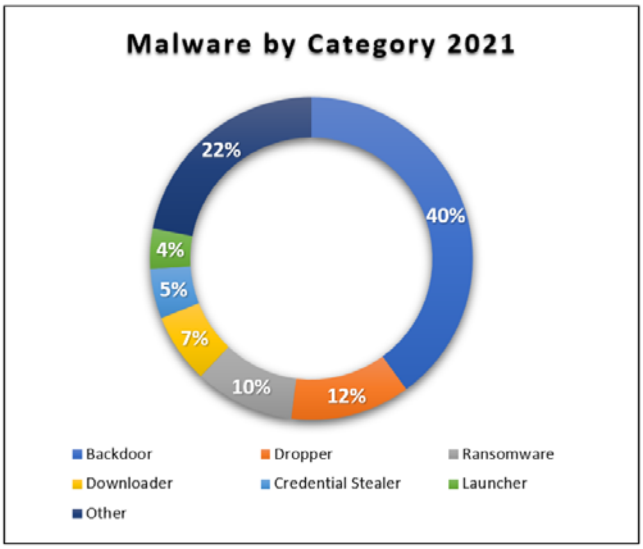

Figure 1 Malware by Category 2021

Only in 2021, Mandiant observed 733 malware families, and the five top categories were: backdoors (40%), droppers (12%), ransomware (10%), downloaders (7%), and credential stealers (5%).

Analysis of Technics, Tactics, and Procedures (TTPs) used by threat actors shows that the five most used techniques, according to MITRE ATT&CK systematics, are:

- T1027: Obfuscated Files or Information - 51.4%
- T1059: Command and Scripting Interpreter - 44.9%
- T1071: Application Layer Protocol - 36.8%
- T1082: System Information Discovery - 31.8%
- T1083: File and Directory Discovery - 31.7%

And top five most frequent sub-techniques cover:

- T1071.001: Web Protocols 32.0%
- T1059.001: PowerShell 29.4%
- T1070.004: File Deletion 27.1%
- T1569.002: Service Execution 26.5%
- T1021.001: Remote Desktop Protocol 23.4%

Advanced Persistent Threat Kill Chain covers more steps than classical seven stages kill chains. In the case of APT or Targeted Attack Lifecycle, we can distinguish:

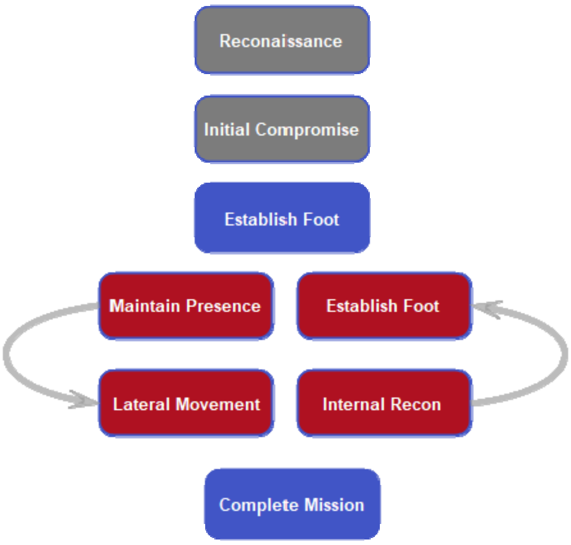

Figure 2. Targeted Attack Cyber Kill Chain

In 2021 threat actors are using new techniques, tactics, and procedures to deploy malware rapidly and efficiently through a business environment. Many attackers target VMWare vSphere and ESXi platform and vCenter Server. Most used tools cover Apache Log4j exploitation (CVE-2021-44228). It is worth noting that in 2020 VMware solutions were used by 25,8% of all virtualization markets.

Since the first group APT1 PLA (People's Liberation Army) Unit 61398, was reported by Mandiant in 2013, in 2021, they observed the actions of 36 APT Chinese groups. Moreover, between 2016 and 2021 activity of 244 distinct Chinese cyber espionage threat actors are observed. Concerted efforts by the US, UK, and other European governments allow for detection and link to China's extensive espionage operations, including exploitation of Microsoft Exchange servers and ransomware campaigns.

Mandiant found out that most of the compromises that affected the observed system were caused by on-premises misconfigurations, lack of strong password and least-privilege principle, privileged user account usage on unnecessary assets, GPO edit permission for non-privileged users, use of account delegation, and Microsoft Certificate Authority misconfiguration. On Microsoft Azure and Microsoft 365 cloud solutions, most risk is concentrated on the lack of MFA or its relaxed use. Even if MFA is appropriately configured, the use of some commonly known legacy authentication protocols such as IMAP4, Autodiscover, Exchange Active Sync (EAS), POP3, Outlook Anywhere, Active Sync, or Authenticated SMTP allows attackers to bypass MFA mechanisms.

Cloud-based services are commonly used across the entire world economy. The US Coast Guard reports that they noticed a significant trend in the transition to cloud-based email and office productivity services in the Maritime Environment – 85% of observed organizations use cloud-based email solutions.

The same problems Mandiant observed are reported in the annual US Coast Guard Report [4], [15]. That is a lack of Least Privilege Principles, a lack of Strong Password Policy, or a lack of MFA. The authors state that the problem of insufficient Patch Management Policy or misconfigurations problem is utilized by APT actors that target Maritime Environment and often gain access by targeting company users with methods such as Phishing for Information or by Compromising Systems with Known Exploitable Vulnerabilities (KEV). In 2022 there was a 20% increase in cyber incident reporting compared to 2021. The Coast Guard Cyber Protection Teams (CPTs) reported the identification of 139 known exploitable vulnerabilities during 2022 missions. They discovered over 3000 hashes of easily crackable passwords with less than 13 characters. That means we must work hard to improve the cyber security landscape posture in Maritime Environments.

While 90% of US imports and exports flow through Maritime Environments, which is more than 5.4 trillion USD, the ME is constantly targeted by APT and Financially motivated Threat Actors [16]–[19]. The Threat Actors in these cases often utilize well-known TTP and USCG Reports showing that Phishing (T1598) and Valid Accounts (T1078) were the most frequently observed technics. The Coast Guard Cyber Protection Teams emulate attacks by using well-known TTP:

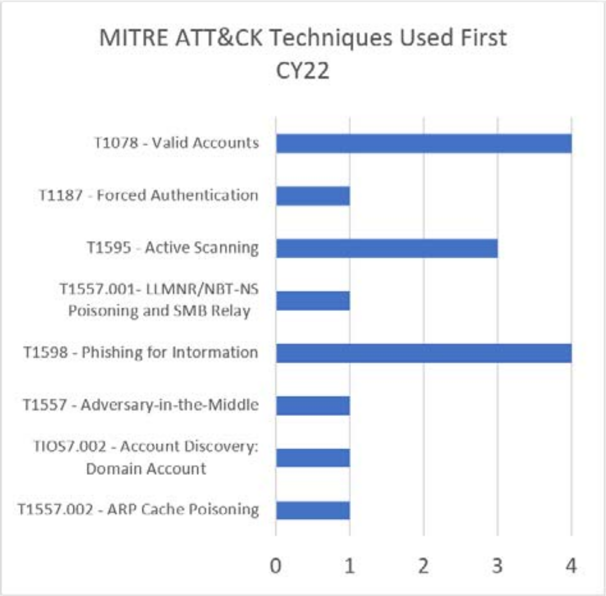

Figure 3. MITRE ATT&CK Techniques Used First CY22. Developed based on [15]

The password hashes used for Brute Force were obtained using: LLMNR/NBT-NS Poisoning, SMB Relay, Steal or Forge Kerberos Tickets: Kerberoasting and Credential Dumping sub-techniques.

The achieved result shows improvements in the mitigations of the risks.

Table 1. Mitigation Status 2021 vs 2022

All Findings	CY21	CY22
Fully Mitigated	48%	62% ↑
Partially Mitigated	33%	31% ↓
Accepted Risk	5%	0% ↓
False Positive	2%	0% ↓
No Action Taken to Date	12%	8% ↓

Developed based on [15]

One of the most common and dangerous threats – ransomware attacks, evolved in the last years. The current trends show three disturbing trends which can be observed in a variety of organizations, including Maritime. First – Victim Shaming - attackers use multi-extorsion technics to ensure organizations pay a ransom demand. Releasing samples of victims' data on the darknet, including details on the total amount of data trying to shame victims into payment. So far, criminals have encrypted organizations' files, and now they leverage leak sites and threaten follow-on DDoS attacks. The second trend is using Ransomware-as-a-Service for ransomware campaigns which quickly lowers the technical skills required for such attacks. And the third aspect is the numerous and extensive use of Zero-Days vulnerabilities in ransomware attacks [20].

At the 2022 Cyber-SHIP Lab conference, researchers from the University of Plymouth presented a simulated attack on Port of New York and New Jersey. It is the largest port on the United States East Coast and the third largest in the US. The simulated attack started with sending a fake phishing email regarding an urgent electronic chart update and finished with the targeted vessel's complete blockage of the fairway. Malware hidden in the update managed to take control of the ship's engine and rudder and disabled any control signals from the ship's bridge at the designated geographical position. Simulation shows that in case of such attacks, crew members were utterly helpless, and in one minute and thirty seconds, the traffic in one of the most sensitive points of the fairway was blocked. The expected losses have been estimated at 180 million dollars in the first six hours [21]. That was only a simulated incident; however, the Ever Given container ship Suez Canal grounding incident [22] shows the impact of such an incident on the worldwide economy.

4 CONCLUSIONS

The ongoing conflict in Ukraine and the cyberattacks carried out as part of it show the meaning of cyber security and cyber resilience in the nowadays worldwide economy. Numerous cyber incidents in Maritime Environment [16], [17], [19], [23]–[28] clearly show how much has to be done to achieve desired resiliency level. Activity of the APT nation-state or state-sponsored groups observation is constantly increasing, and due to the complexity of the Maritime Environment, threats to the maritime industry continue to grow.

REFERENCES

[1] "CrowdStrike 2023 Global Threat Report | Executive Summary," crowdstrike.com. https://www.crowdstrike.com/resources/reports/global-threat-report-executive-summary-2023/ (accessed June 14, 2023).

[2] "M-Trends 2022: Cyber Security Metrics, Insights and Guidance From the Frontlines," Mandiant. https://www.mandiant.com/resources/blog/m-trends-2022 (accessed June 14, 2023).

[3] K. Monica, S. James, and S. Max, "The Cyber Operations during the 2022 Russian invasion of Ukraine: Lessons Learned (so far)," Jul. 2022. [Online]. Available: https://eccri.eu/wp-content/uploads/2022/07/ECCRI_WorkshopReport_Version-Online.pdf

[4] "2021 Cyber Trends and Insights in the Marine Environment (CTIME) Report," Aug. 2022. Accessed: June 14, 2023. [Online]. Available: https://safety4sea.com/uscg-cyber-trends-and-insights-in-the-marine-environment/

[5] B. Svilicic, K. Junzo, M. Rooks, and Y. Yano, "Maritime Cyber Risk Management: An Experimental Ship Assessment," J. Navig., vol. 72, pp. 1–13, Feb. 2019, doi: 10.1017/S0373463318001157.

[6] M. Maynes, "One simple action you can take to prevent 99.9 percent of attacks on your accounts," Microsoft Security Blog, August 20, 2019. https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/ (accessed June 14, 2023).

[7] D. Freeze, "Multi-Factor Authentication Is (Not) 99 Percent Effective," Cybercrime Magazine, February 23, 2023. https://cybersecurityventures.com/multi-factor-authentication-is-not-99-percent-effective/ (accessed June 14, 2023).

[8] "Hacking Two Factor Authentication: Four Methods for Bypassing 2FA and MFA – The CISO Perspective," January 13, 2022. https://cisoperspective.com/index.php/2022/01/13/hacking-two-factor-authentication-four-methods-for-bypassing-2fa-and-mfa/ (accessed June 14, 2023).

[9] "CVE - CVE-2021-32648." https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-32648 (accessed June 14, 2023).

[10] Editorial, "Ukraine banking and defense platforms knocked out amid heightened tensions with Russia," NetBlocks, February 15, 2022. https://netblocks.org/reports/ukraine-banking-and-defence-platforms-knocked-out-russia-conflict-JBQX7mAo (accessed June 14, 2023).

[11] https://news.viasat.com/viasat, "KA-SAT Network cyber attack overview," viasat.com, March 30, 2022. https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview (accessed June 14, 2023).

[12] "2022 Ukraine cyberattacks," Wikipedia. May 04, 2023. Accessed: June 14, 2023. [Online]. Available: https://en.wikipedia.org/w/index.php?title=2022_Ukraine_cyberattacks&oldid=1153205698

[13] State of the Hack: One Year after the APT1 Report, (February 28, 2014). Accessed: June 14, 2023. [Online Video]. Available: https://www.youtube.com/watch?v=88o-uifbJSE

[14] "Internet Crime Complaint Center(IC3) | Annual Reports." https://www.ic3.gov/Home/AnnualReports (accessed June 14, 2023).

[15] Coast Guard Cyber Command, "2022 Cyber Trends and Insights in the Marine Environment (CTIME) Report," United States Coast Guard, May 2023. [Online]. Available: https://www.uscg.mil/Portals/0/Images/cyber/2022CTIMEReport_Final.pdf?ver=lFYiLZqt4dbVf2RFTgL15g%3d%3d&timestamp=1685643398263

[16] A. Ajdin, "Hapag-Lloyd flags spear phishing attack," Splash247, March 08, 2022. https://splash247.com/hapag-lloyd-flags-spear-phishing-attack/ (accessed June 15, 2023).

[17] "Phishing impersonates shipping giant Maersk to push STRRAT malware," BleepingComputer. https://www.bleepingcomputer.com/news/security/phishing-impersonates-shipping-giant-maersk-to-push-strrat-malware/ (accessed June 15, 2023).

[18] "Cyberattack Threatens Release of Port of Lisbon Data," The Maritime Executive. https://maritime-executive.com/article/cyberattack-threatens-release-of-port-of-lisbon-data (accessed June 15, 2023).

[19] "Voyager Worldwide hit by cyber attack - Splash247." https://splash247.com/voyager-worldwide-hit-by-cyber-attack/ (accessed June 15, 2023).

[20] Unit 42, "2022 Unit 42 Ransomware Threat Report Highlights: Ransomware Remains a Headliner," Unit 42, March 24, 2022. https://unit42.paloaltonetworks.com/2022-ransomware-threat-report-highlights/ (accessed June 14, 2023).

[21] "Cyber-SHIP Lab Annual Symposium," University of Plymouth, November 01, 2023. https://www.plymouth.ac.uk/whats-on/cyber-ship-lab-annual-symposium (accessed June 16, 2023).

[22] "Ever Given," Wikipedia. May 31, 2023. Accessed: June 16, 2023. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Ever_Given &oldid=1157809412

[23] "Ransomware attack on maritime software impacts 1,000 ships." https://therecord.media/ransomware-attack-on-maritime-software-impacts-1000-ships (accessed June 14, 2023).

[24] S. Lyngaas, "Hackers breached computer network at key US port but did not disrupt operations | CNN Politics," CNN, September 23, 2021. https://www.cnn.com/2021/09/23/politics/suspected-foreign-hack-houston/index.html (accessed June 14, 2023).

[25] "Spoofing in the Black Sea: What really happened?," GPS World, October 11, 2017. https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/ (accessed June 12, 2023).

[26] "GPS freaking out? Maybe you're too close to Putin," NRKbeta, September 18, 2017. https://nrkbeta.no/2017/09/18/gps-freaking-out-maybe-youre-too-close-to-putin/ (accessed June 12, 2023).

[27] T. Neumann (2017). Automotive and telematics transportation systems. Paper presented at the 2017 International Siberian Conference on Control and Communications, SIBCON 2017 - Proceedings, doi:10.1109/SIBCON.2017.7998555

[28] A. Weintrit, T. Neumann (2019). Advances in marine navigation and safety of sea transportation. introduction. Advances in Marine Navigation and Safety of Sea Transportation - 13th International Conference on Marine Navigation and Safety of Sea Transportation, TransNav 2019.